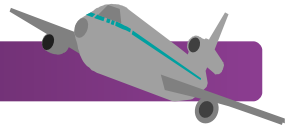


Digital Signature

Educating The Traveler

Lesson Plan

Defense Travel System Training Program

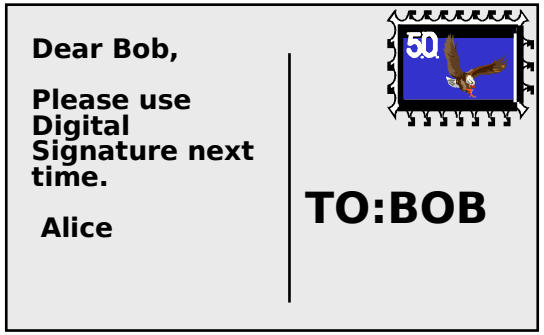
- ✓ Features
- ✓ Components
- ✓ How to register
- ✓ Use of Digital Signature
- ✓ Help

Digital Signature Features

Defense Travel System Training Program

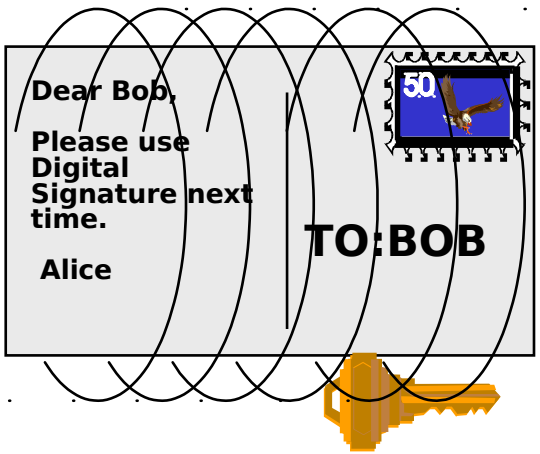
WITHOUT Digital Signature

- No Identification & Authentication

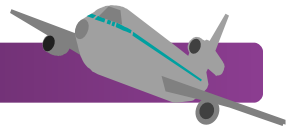


WITH Digital Signature

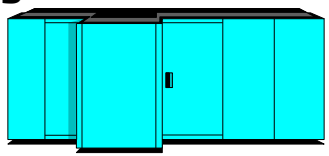
- Provides Identification & Authentication
- "Non-repudiation"



DTS
PKI Components



- **Certification Authority (CA):**
  - **Certificate Server that creates and signs certificates**

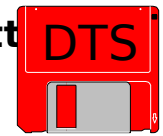


- **DoD Directory:**
  - maintains certificate for validation and certificate revocation list

- **Registration Authority (RA):**
  - **Manage Local Registration Authority**
  - **Revocation Authority**

- **Local Registration Authority (LRA):**
  - **Register users with the CA**
  - **Provides DOD PKI information to us**

- **Traveler's Key Storage: Diskett**



Registering the Traveler

Defense Travel System Training Program

1. Traveler contacts LRA to register in the system.

2. LRA records personnel information of the User.

3. Traveler obtains certificate registration instructions with user number, password* and WEB address.

* One-time password - Used only once to access the PKI or

Registering the Traveler (cont'd)

4. LRA submits the User's personnel info to the PKI system.

5. User logs on to the system using the User Number and password.*

6. LRA records the User's Unique Identification Number (UIN) to be used by the Defense Travel Administration (DTA) for DTS access control.

* **If three (3) unsuccessful attempts are made to log on, use will be locked out - must contact LRA to access the accoun**

FOR TRAINING ONLY

DoD Public Key Infrastructure (PKI)
Certificate Registration Instructions

Require Photo ID before hand Delivery to:
Joe Test:
Time Sensitive Material
Certificate Registration Instructions

Please read this sheet very carefully, and follow the instructions on it. Please DO NOT allow anyone to see the password on th have completed the process described below! This page will help you to obtain your personal digital certificate. Others will us electronically identify you. If you have any problems or questions, please notify your "Local Registration Authority," who is

Jamil J. Nimeh
619-552-5403
DSN: 619-552-5112
jamil.j.nimeh@cpmx.saic.com

You Must register within thirty days. Please have a floppy disk ready. You will need it to store your digital certificate. With a w in the "Netsite" or "Open Page" space

ds-2.den.disa.mil

and follow the instructions on that web site. (Please note that, at present, you must use the US version of Netscape Navigato 4.05 or later. In the future, other brands will also be supported.)

You will be asked to compare a "Certificate Fingerprint". Ensure it is: 52:A5: D3:C9: 19:84: FE:CF:A4:AD:AE:69:33:36:95:6D

When asked by the web site to select a Certificate Authority, select CA-I. Later, you will be asked to fill in your User Number a This password will only be used once, so you do not need to remember it.

Your User Number: 0008000108
Your Password: YAdAC6eD

This is government information for official use only. Access to this information requires compliance to DoD standards and regu statues and regulations provide penalties for unauthorized access or use of this information.

FOR TRAINING ONLY

Requesting a Digital Signature Certificate

Defense Travel System Training Program

1. Access the designated PKI server by connecting to the Netscape Internet browser, and typing in the web address that was given to you by your LRA (on Identity Certificate Registration form)

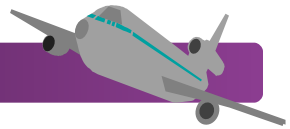
2. Fill out the form and submit reque

3. Click OK to generate private key.

4. Enter password and click on OK.

DTS Use of Digital Signature

Defense Travel System Training Program



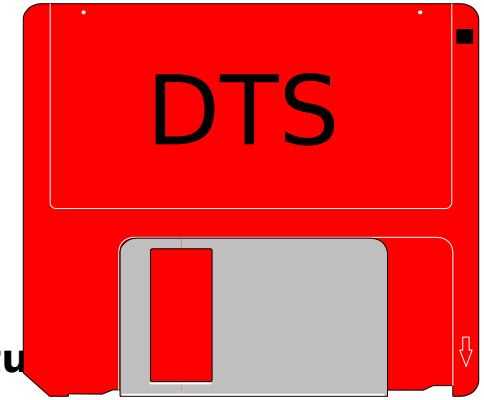
1. Required to access the CUI

2. Traveler signs authorization request

3. Authorizing Official (AO) authorizes travel

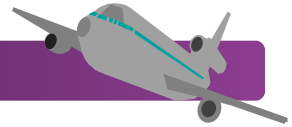
4. Traveler signs travel authorization after trip with actu
   expenses

5. AO signs approving payment (Certifying Official if not AO would have to sign to approve payment)



Registration Process

Defense Travel System Training Program



1

Local Registration Authority

2

Prepare User Registration

Web-Based

Public Key

Web-Based Certification Authority

One-Time Password

3

4

6

Auto

CERT

5

DTS

Private Key

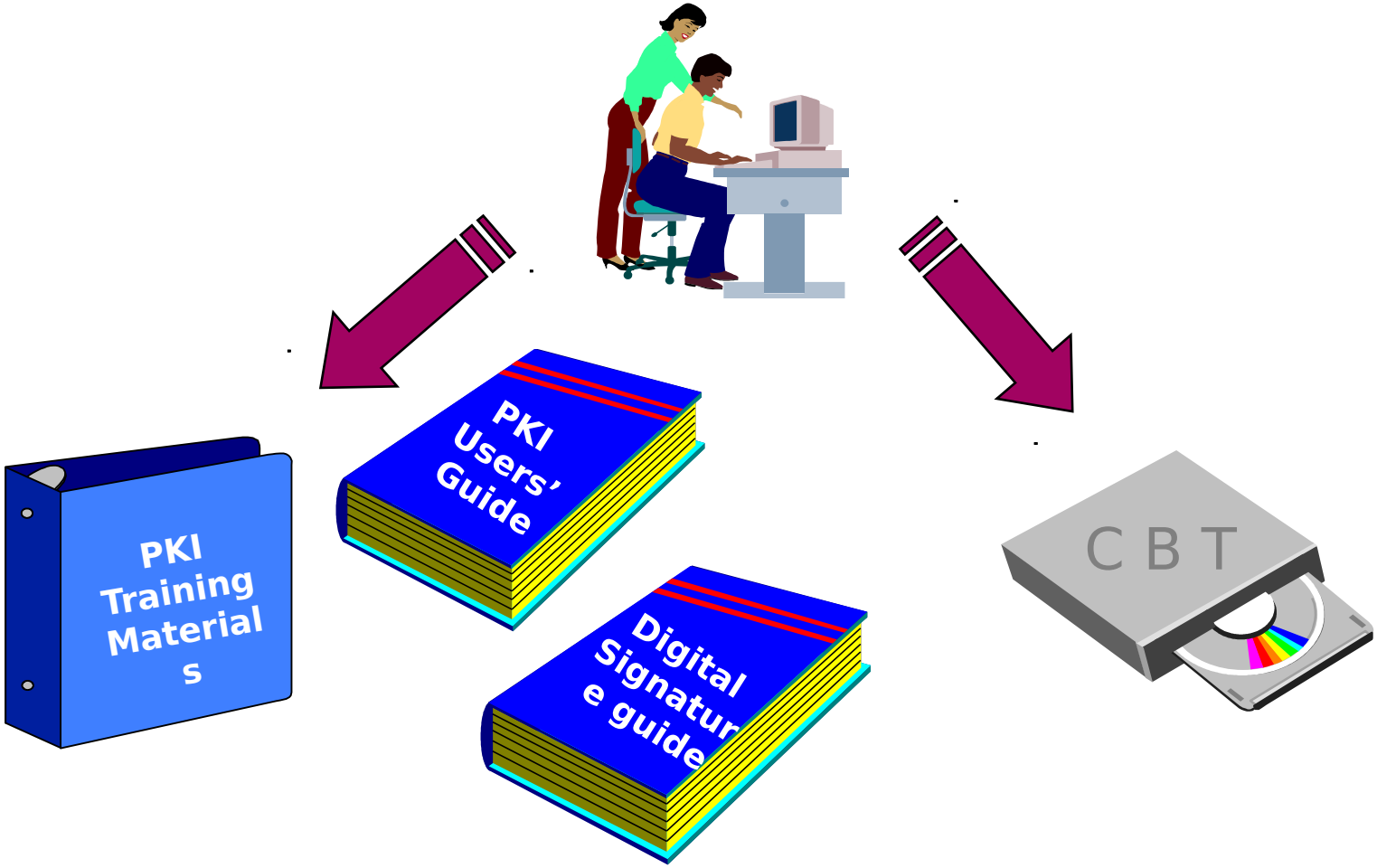
User

DOD Directory Services

DOD Medium Assurance PKI Infrastructure

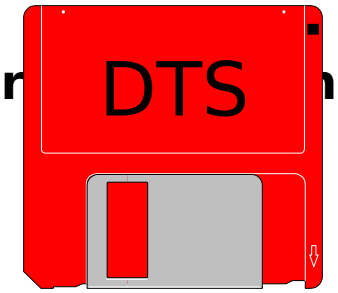
Where To Go For Help

Contact Your LRA for Assistance



Digital Signature Security

- ✓ Keep password from Certificate Registration Instructions page (from LRA) safe until registration
- ✓ Register on-line via Netscape browser to create digital signature certificate (save to diskette)
- ✓ Delete private key from hard drive after creating
- ✓ KEEP YOUR DISKETTE SAFE!!
  - Unclassified - Treat as a credit or bank card
  - Remember your Password
  - Write protect diskette
- ✓ DO NOT store non-digital signature information on your diskette
- ✓ Use diskette as dir[illegible] requested by the DTS application



Questions?